Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A cryptographic device for securing data on a computer network comprising:

a processor programmed to authenticate a plurality of users on the computer network for secure processing of a value bearing item, wherein the processor includes a state machine for determining a state corresponding to availability of one or more commands;

a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users;

a cryptographic engine for cryptographically protecting data; and

an interface for communicating with the computer network;

wherein the cryptographic device is located remotely from the plurality of users; and

wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user.

2. (Original) The cryptographic device of claim 1, wherein the state machine includes an uninitialized state.

3. (Original) The cryptographic device of claim 1, wherein the state machine includes an initialized state.

4. (Original) The cryptographic device of claim 1, wherein the state machine includes an operational state.

5. (Original) The cryptographic device of claim 1, wherein the state machine includes an administrative state.

6. (Original) The cryptographic device of claim 1, wherein the state machine includes an exporting shares state.

7. (Original) The cryptographic device of claim 1, wherein the state machine includes an importing shares state.

8. (Original) The cryptographic device of claim 1, wherein the state machine includes an error state.

9. (Original) The cryptographic device of claim 2, wherein the one or more commands corresponding to the uninitialized state includes a command for start initializing.

10. (Original) The cryptographic device of claim 3, wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands.

11. (Original) The cryptographic device of claim 4, wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support.

12. (Original) The cryptographic device of claim 11, wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command.

13. (Original) The cryptographic device of claim 11, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

14. (Original) The cryptographic device of claim 11, wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands.

15. (Original) The cryptographic device of claim 11, wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command.

16. (Original) The cryptographic device of claim 5, wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command.

17. (Original) The cryptographic device of claim 6, wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command.

18. (Original) The cryptographic device of claim 7, wherein the one or more commands corresponding to the importing shares state include commands for one or more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command.

19. (Original) The cryptographic device of claim 8, wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command.

20. (Original) The cryptographic device of claim 1 further comprising computer executable code to keep track of a present operational state.

21. (Original) The cryptographic device of claim 1, wherein the processor is programmed to verify that the authenticated user is authorized to assume a role and perform a corresponding operation.

22. (Original) The cryptographic device of claim 1, wherein the cryptographic device includes a computer executable code for preventing unauthorized disclosure of data.

23. (Original) The cryptographic device of claim 1, wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

24. (Original) The cryptographic device of claim 1, wherein the value bearing item is a postage value including a postal indicium.

25. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises a digital signature.

26. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises a postage amount.

27. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

28. (Original) The cryptographic device of claim 1, wherein the value bearing item is a ticket.

29. (Original) The cryptographic device of claim 1, wherein the value bearing item includes a bar code.

30. (Original) The cryptographic device of claim 1, wherein the value bearing item is a coupon.

31. (Original) The cryptographic device of claim 1, wherein the value bearing item is currency.

32. (Original) The cryptographic device of claim 1, wherein the value bearing item is a voucher.

33. (Original) The cryptographic device of claim 1, wherein the value bearing item is a traveler's check.

34. (Previously presented) The cryptographic device of claim 1, wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

35. (Original) The cryptographic device of claim 1, wherein each security device transaction data includes

information to define the present operational state of the device.

36. (Original) The cryptographic device of claim 1, wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices.

37. (Original) The cryptographic device of claim 1, wherein the processor and the cryptographic engine generate a master key set (MKS).

38. (Original) The cryptographic device of claim 37, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

39. (Original) The cryptographic device of claim 38, wherein the MKS further includes a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

40. (Original) The cryptographic device of claim 1, wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

41. (Original) The cryptographic device of claim 1, wherein at least one of the plurality of users is an enterprise account.

42. (Currently Amended) A method for securing data on a computer network including a plurality of remotely-located users comprising the steps of:

authenticating the plurality of users for secure processing of a value bearing item using one of a plurality of cryptographic devices;

storing security device transaction data in a memory for ensuring authenticity and authority of one of the plurality of users, wherein the security device transaction data is related to the one of the plurality of users;

determining a state in a state machine for availability of one or more commands; and

once the user is authenticated, entering an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user.

43. (Original) The method of claim 42 further comprising the step of printing the value bearing item.

44. (Original) The method of claim 42 further comprising the step of storing a plurality of security device transaction data in a database wherein, each transaction data is related to one of the plurality of users.

45. (Original) The method of claim 44 further comprising the step of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item.

46. (Original) The method of claim 42 further comprising the steps of authenticating the identity of each user and

verifying that the identified user is authorized to assume a role and to perform a corresponding operation.

47. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an uninitialized state.

48. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an initialized state.

49. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an operational state.

50. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an administrative state.

51. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an exporting shares state.

52. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an importing shares state.

53. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an error state.

54. (Original) The method of claim 47, wherein the one or more commands corresponding to the uninitialized state includes a command for start initializing.

55. (Original) The method of claim 48, wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands.

56. (Original) The method of claim 49, wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support.

57. (Original) The method of claim 56, wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command.

58. (Original) The method of claim 56, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

59. (Original) The method of claim 56, wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands.

60. (Original) The method of claim 56, wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command.

61. (Original) The method of claim 50, wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command.

62. (Original) The method of claim 51, wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command.

63. (Original) The method of claim 52, wherein the one or more commands corresponding to the importing shares state

include commands for one or more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command.

64. (Original) The method of claim 53, wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command.

65. (Original) The method of claim 42, further comprising the step of printing a postage value including a postal indicium.

66. (Original) The method of claim 65, wherein the postal indicium includes a digital signature.

67. (Original) The method of claim 65, wherein the postal indicium includes a postage amount.

68. (Original) The method of claim 65, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

69. (Original) The method of claim 42, further comprising the step of printing a ticket.

70. (Original) The method of claim 42, further comprising the step of printing a bar code.

71. (Original) The method of claim 42, further comprising the step of printing a coupon.

72. (Currently Amended) A security system for securing data in a computer network comprising:

a plurality of user terminals coupled to the computer network;

a plurality of cryptographic device remote from the plurality of user terminals and coupled to the computer network, wherein one of the plurality of cryptographic devices manages value available to users and includes a state machine for determining a state corresponding to one or more commands available to an authenticated user; and

a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user; and

wherein, once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user for one or more transactions requested by the user.

73. (Currently Amended) The system of claim 72, wherein the security device transaction data related to a user is loaded into the one of the plurality cryptographic devices when the user requests to operate on a value bearing item.

74. (Original) The system of claim 72, wherein the state machine includes an uninitialized state.

75. (Original) The system of claim 72, wherein the state machine includes an initialized state.

76. (Original) The system of claim 72, wherein the state machine includes an operational state.

77. (Original) The system of claim 72, wherein the state machine includes an administrative state.

78. (Original) The system of claim 72, wherein the state machine includes an exporting shares state.

79. (Original) The system of claim 72, wherein the state machine includes an importing shares state.

80. (Original) The system of claim 72, wherein the state machine includes an error state.

81. (Original) The system of claim 74, wherein the one or more commands corresponding to the uninitialized state includes a command for start initializing.

82. (Original) The system of claim 75, wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands.

83. (Original) The system of claim 76, wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support.

84. (Original) The system of claim 83, wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command.

85. (Original) The system of claim 83, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

86. (Original) The system of claim 83, wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands.

87. (Original) The system of claim 83, wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command.

88. (Original) The system of claim 77, wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff

command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command.

89. (Original) The system of claim 78, wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command.

90. (Original) The system of claim 79, wherein the one or more commands corresponding to the importing shares state include commands for one or more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command.

91. (Original) The system of claim 80, wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command.

92. (Original) The system of claim 72 further comprising computer executable code to keep track of a present operational state.

93. (Original) The system of claim 72, wherein the processor is programmed to verify that the authenticated user is

authorized to assume a role and perform a corresponding operation.

94. (Original) The system of claim 72, wherein the system includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

95. (Original) The system of claim 72, wherein the value bearing item is a postage value including a postal indicium.

96. (Original) The system of claim 95, wherein the postal indicium comprises a digital signature.

97. (Original) The system of claim 95, wherein the postal indicium comprises a postage amount.

98. (Original) The system of claim 95, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

99. (Original) The system of claim 72, wherein the value bearing item is a ticket.

100. (Original) The system of claim 72, wherein the value bearing item includes a bar code.

101. (Original) The system of claim 72, wherein each security device transaction data includes information to define the present operational state of the device.

102. (Original) The system of claim 72, wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

103. (Original) The system of claim 72, wherein at least one of the users is an enterprise account.

104. (Currently Amended) A method for secure printing of value-bearing items over a computer network having a plurality of user terminals, the method comprising the steps of:

storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of user terminals;

securing the information about the users in the database by one or more of a plurality of cryptographic devices remote from the plurality of user terminals, wherein each of the cryptographic devices manages value available for the value bearing items;

storing a plurality of security device transaction data in the database, wherein each transaction data is related to one of the plurality of users; and

determining a state in a state machine for availability of one or more commands;

continuing to authenticate individual user transaction requests even after a user has been authorized by the cryptographic device.

105. (Original) The method of claim 104 further comprising the step of printing the value bearing item.

106. (Currently Amended) The method of claim 104 further comprising the step of loading a security device transaction data related to a user into one of the one or more of the plurality of cryptographic devices when the user requests to operate on a value bearing item.

107. (Original) The method of claim 104 further comprising the step of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item.

108. (Original) The method of claim 104 further comprising the steps of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation.

109. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an uninitialized state.

110. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an initialized state.

111. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an operational state.

112. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an administrative state.

113. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an exporting shares state.

114. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an importing shares state.

115. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an error state.

116. (Original) The method of claim 104, further comprising the step of printing a postage value including a postal indicium.

117. (Original) The method of claim 116, wherein the postal indicium includes a digital signature.

118. (Original) The method of claim 116, wherein the postal indicium includes a digital signature.

119. (Original) The method of claim 116, wherein the postal indicium includes a postage amount.

120. (Original) The method of claim 104, further comprising the step of printing a ticket.